

Vectorizing Higher-Order Masking

Benjamin Grégoire, Kostas Papagiannopoulos, Peter Schwabe, and
Ko Stoffelen



Motivation

- Masking is a popular side-channel analysis countermeasure
 - Split variables into shares
 - Amplifies noise
- Higher-order masking...
 - ... makes attack harder
 - ... makes implementation much slower
- Bounded moment leakage model studies parallel masking [BDF+17]
- This work:
 - Exploit NEON vector registers on Cortex-A8 for faster parallel 4-share and 8-share bitsliced AES
 - Evaluate its security against side-channel analysis



ARM NEON vector registers

- Cortex-A8 is widely deployed, comes with NEON Advanced SIMD
 - 16×128 -bit register *or* 32×64 -bit register
- Bitsliced AES needs 8×16 bits



Secure parallel refreshing/multiplication

- Gadgets should be *composable*, requires strong non-interference (SNI) [BBD⁺16]
- Program verification used to prove SNI and security in model
- Refreshing
 - 4 shares $\mathbf{r} \quad \text{rot}(\mathbf{r}, 1) \quad \mathbf{x}$
 - 8 shares $\mathbf{r} \quad \text{rot}(\mathbf{r}, 1) \quad \mathbf{r} \quad \text{rot}(\mathbf{r}, 2) \quad \mathbf{x}$
- Multiplication
 - 4 shares
$$\mathbf{x} \cdot \mathbf{y} \quad \mathbf{r} \quad \mathbf{x} \cdot \text{rot}(\mathbf{y}, 1) \quad \text{rot}(\mathbf{x}, 1) \cdot \mathbf{y} \quad \text{rot}(\mathbf{r}, 1) \quad \mathbf{x} \cdot \text{rot}(\mathbf{y}, 2)$$
$$[r, r, r, r]$$
 - 8 shares
$$\mathbf{x} \cdot \mathbf{y} \quad \mathbf{r} \quad \mathbf{x} \cdot \text{rot}(\mathbf{y}, 1) \quad \text{rot}(\mathbf{x}, 1) \cdot \mathbf{y} \quad \text{rot}(\mathbf{r}, 1)$$
$$\mathbf{x} \cdot \text{rot}(\mathbf{y}, 2) \quad \text{rot}(\mathbf{x}, 2) \cdot \mathbf{y} \quad \mathbf{r}$$
$$\mathbf{x} \cdot \text{rot}(\mathbf{y}, 3) \quad \text{rot}(\mathbf{x}, 3) \cdot \mathbf{y} \quad \text{rot}(\mathbf{r}, 1)$$
$$\mathbf{x} \cdot \text{rot}(\mathbf{y}, 4) \quad \mathbf{r} \quad \text{rot}(\mathbf{r}, 1)$$



Randomness (bytes)

	4 shares	8 shares
Refreshing	8	32 (was 48)
Multiplication	10 (was 16)	48
Full AES	5,760	25,600

Speed of RNG has large impact on performance!



Performance

	4 shares 1 block	4 shares 2 blocks	8 shares 1 block
Clock cycles (rand. from /dev/urandom)	1,598,133	4,738,024	9,470,743
Clock cycles (rand. from normal file)	14,488	17,586	26,601
Clock cycles (pre-loaded rand.)	12,385/ 774 cpb	15,194/ 475 cpb	23,616/ 1476 cpb
Stack usage in bytes	12	300	300
Code size in bytes	39,748	44,004	70,188



SCA evaluation setup



SCA evaluation setup

- BeagleBone Black @ 1 GHz, running Debian
- LeCroy WaveRunner @ 2.5 GS/s for 1M traces
- Langer EM probe RF-B 0.3-3 @ capacitor 66
- Langer amplifier PA 303 SMA
- Trigger using GPIO port
- Data over Ethernet/TCP
- Elastic alignment post-processing [[vWWB11](#)]

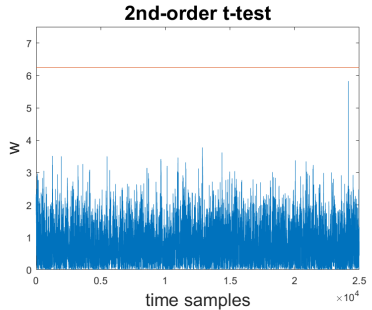
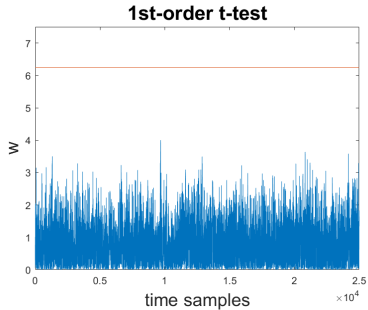


Share independence

- Ideally, d -share schemes are secure against $(d - 1)$ -order attacks
- Share recombination, coupling effects, distance-based leakage cause divergence
- Practical security order $< d - 1$
- Order reduction theorem: practical security order $\frac{d-1}{2}$ [BGG⁺14]
- So when $d = 4$, 1st order security?

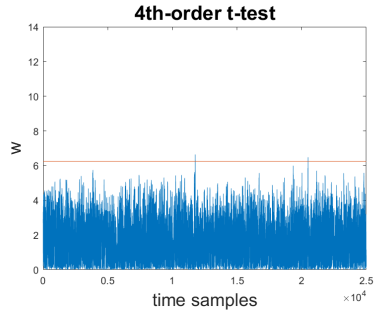
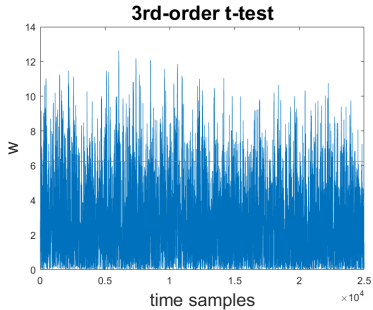


TVLA



T-test suggests resistance against 2st order attacks

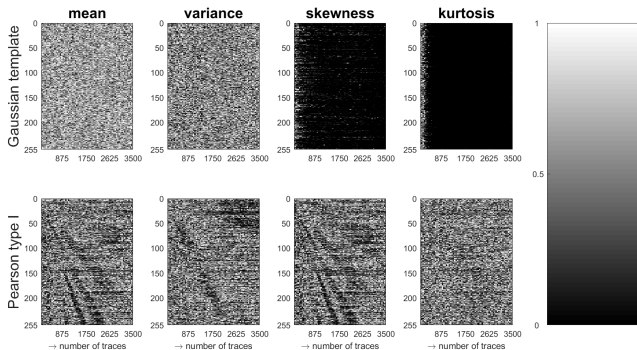
TVLA



Security issues at 3rd order

Leakage certification

- Two types of errors [DSDP16]
 - Estimation errors: not enough traces
 - Modelling errors: incorrect leakage assumption
- Leakage certification can distinguish between them



Information-theoretic bounds

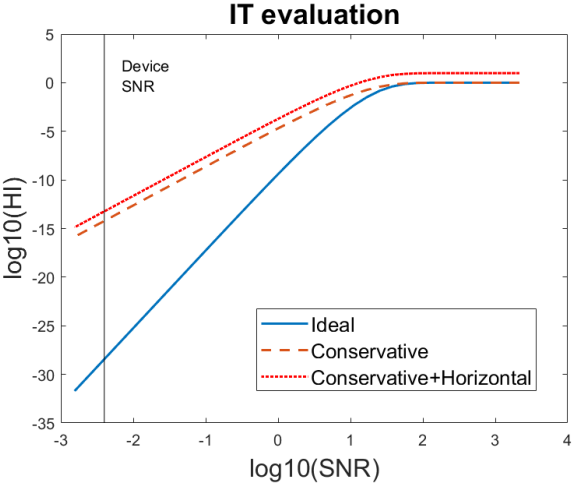
- How to evaluate an 8-share implementation? [DFS15]
 1. Estimate the SNR of the device ($= 0.004$)
 2. Compute the hypothetical information between the leakage and the secret key

$$H(S; L) = H[S] + \sum_s \Pr[s] \sum_{\ell} \Pr[\ell / s] \cdot \log_2 \Pr_{\text{model}}[s / \ell]$$

3. Extrapolate to 8 shares using information theoretical bounds



Information-theoretic bounds



Conclusions

- ARM NEON is a powerful tool for implementors
- Parallellized implementations become increasingly relevant in the context of SCA countermeasures
- Ensuring share independence seems to be hard and interfaces with the architectural and electrical layers
- Understanding the randomness requirements for masking / an efficient masking RNG is still an important open problem



Thanks...

... for your attention!

Questions?



References I



Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rébecca Zucchini.

Strong non-interference and type-directed higher-order masking.

In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pages 116–129. ACM, 2016.

<http://epri.nt.iacr.org/2015/506.pdf>.



Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub.

Parallel implementations of masking schemes and the bounded moment leakage model.

In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology — EUROCRYPT 2017*, volume 10210 of *LNCS*, pages 535–566. Springer, 2017.

<http://epri.nt.iacr.org/2016/912.pdf>.



Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, and François-Xavier Standaert.

On the cost of lazy engineering for masked software implementations.

In Marc Joye and Amir Moradi, editors, *Smart Card Research and Advanced Applications — CARDIS 2014*, volume 8968 of *LNCS*, pages 64–81. Springer, 2014.

<http://epri.nt.iacr.org/2014/413.pdf>.



References II



Alexandre Duc, Sebastian Faust, and François-Xavier Standaert.
Making masking security proofs concrete — Or how to evaluate the security of any leaking device.
In *Advances in Cryptology — EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 401–429. Springer, 2015.
<https://eprint.iacr.org/2015/119.pdf>.



François Durvaux, François-Xavier Standaert, and Santos Merino Del Pozo.
Towards easy leakage certification.
In Benedikt Gierlichs and Axel Y. Poschmann, editors, *Cryptographic Hardware and Embedded Systems — CHES 2016*, volume 9813 of *LNCS*, pages 40–60. Springer, 2016.
<https://eprint.iacr.org/2015/537.pdf>.



Jasper G. J. van Woudenberg, Marc F. Witteman, and Bram Bakker.
Improving differential power analysis by elastic alignment.
In Aggelos Kiayias, editor, *Topics in Cryptology — CT-RSA 2011*, *LNCS*, pages 104–119. Springer, 2011.
https://doi.org/10.1007/978-3-642-19074-2_8.

